**U.S DEPARTMENT OF COMMERCE**

**PROCESS GUIDANCE AND MINIMUM IMPLEMENTATION STANDARDS FOR**

# IT System Inventory Management

*[This supersedes the "DOC Guidance for Semi-annual IT System Inventory Updates" v1 issued in February 2003.]*

## What is the purpose of this standard?

The *DOC IT Security Program Policy and Minimum Implementation Standards*, section 3.2.4, establishes the policy for inventory management of IT systems. The Federal Information Security Management Act [FISMA, public law 107-347, Title III, section 3544(b)(5)(A)] amended Title 44 U.S. Code section 3505 to require that agencies establish an inventory of major information systems to support FISMA activities. This standard provides process guidance and minimum implementation requirements for Department of Commerce (DOC) operating unit completion of semi-annual IT system inventory updates. This standard also provides the data dictionary of inventory tables and fields (attachment 1) and provides examples of properly completed inventory forms (attachment 2), for the consistent and comprehensive completion of the semi-annual IT system inventory. Failure to follow the prescribed format and field values as described in this standard will result in inventory updates returned to the operating unit for re-work, and possibly result in the operating unit missing the due date established by IT security policy.

## What is an IT system inventory?

The IT system inventory is a comprehensive list of all national security and non-national security IT systems in the operating unit. It contains IT security program information on each system, and provides a summary of valuable management data that reflects the status of an organization's implementation of its IT Security Program. This inventory also serves as a tool for IT security officers to track compliance with IT security requirements, and for program officials to monitor the operating unit's IT investment portfolio.

## Why must ITSOs submit accurate, complete, and consistent information when updating inventories?

The Federal Information Security Management Act (FISMA – Public Law 107-347, Title III) and the *DOC IT Security Program Policy and Minimum Implementation Standards* require that all operating units maintain a complete and accurate inventory of their IT systems. The Clinger-Cohen Act, and the Office of Management and Budget (OMB) also require in its Circular A-11 that each IT system is tracked and linked to IT capital planning, architecture, and investment control by a unique system identifier number. In addition, the Paperwork Reduction Act establishes a broad mandate for agencies to perform their information resources management activities in an efficient, effective, and economical manner.

The information provided to OMB, members of the U.S. Congress, auditors, and senior management within the operating unit and the Department must be accurate and complete.

Therefore, it is imperative that IT security officers (ITSOs) use the exact values described in the data dictionary (attachment 1) when completing the IT system inventory.

### What is the file format and organization of the IT system inventory?

The IT inventory is a collection of tables of information that can easily be updated or expanded by adding additional tables. The operating units must provide system inventory updates to the Department in Microsoft Excel format (no other file format will be accepted). The Department, in turn, updates its Microsoft Access database using the Excel files. Each table of the unit's inventory can be updated independently, and imported into or exported from the Department's database. The inventory is organized into four tables, as further described in attachment 1. For examples on how to fill out the unit IT security inventory tables, see attachment 2.

### What must be included in the IT system inventory?

The IT system inventory must include IT security program information for all national security and non-national security systems in the operating unit. Definitions for inventory fields, and mandatory field values that must be used for each field, are included in the data dictionary (attachment 1). The IT system inventory must include the following information, shown below by database table, for each system as required by the *DOC IT Security Program Policy and Minimum Implementation Standards*, section 3.2.4. All tables must include each system's System ID, which is assigned by the owning organization's (operating unit or line office) CIO. [*Note: The System ID is the primary key field for all database tables and must be identical in all inventory tables.*]

- The System Description Table contains information that identifies each system. This information includes:
    - The unique descriptive name for each IT system;
    - Sensitivity Type (non-national security or national security);
    - The system's physical location;
    - Type of system (major application or general support system);
    - Life cycle stage (initiation, development/acquisition, implementation, operation/ maintenance, or deactivated/disposed);
    - Deactivation date (if applicable);
    - System criticality (national or mission critical, or business essential);
    - Exhibit 53/300 Account Code(s);
    - System Impact Level (high, moderate, or low); and
    - Operational relationships (government or contractor) of system equipment, facilities, and personnel.
- The System Responsibility Table contains information about individuals who are responsible for the security of each system, including:

- Name and phone of the person assigned security responsibility;
- Name and phone of the system owner; and
- Name and phone of the designated approving authority (responsible operating unit head or delegated senior program official).

- The Security Information Table contains current system security information, reflecting the status of an operating unit's implementation of its IT Security Program. This information is necessary to monitor compliance with IT security requirements and includes:
  - Whether the DOC-modified NIACAP methodology was followed for system C&A;
  - Level of effort applied to the system certification effort;
  - Date the system owner most recently approved the security plan;
  - Date of the last system security risk assessment;
  - Contingency plan date;
  - Date of most recent contingency plan test;
  - Whether a security test & evaluation (ST&E) plan was developed;
  - Date last ST&E plan testing was completed;
  - Date of last system certification;
  - Date of the last system accreditation;
  - The type of accreditation issued;
  - Date of last self assessment completed in accordance with NIST SP 800-26;
  - Dates of most recent three evaluations or audits performed by external organizations within the last 24 months;
  - Names of most recent three external organizations that conducted the evaluations or audits within the last 24 months; and
  - Report numbers of most recent three evaluations or audits within the last 24 months.
- The System Interconnections Table contains information that identifies the interfaces between systems in the inventory and all other systems or networks, including those not operated by or under the control of the Department.
  - Name of the organization to which the system is interconnected
  - System number or name of the interconnected system
  - Type of transaction supported by the interconnection

[NOTE: It is the responsibility of the DOC system owner to establish Service Level Agreements or Memoranda of Understanding for untrusted interconnectivity as well as to obtain and review Certification and Accreditation documentation for all systems to which it will have a trusted interconnection. For more information, see DOC IT Security Program Policy section 3.16.2.2]

### How do you determine the system criticality for each system?

The Department requires that operating units assign a system criticality designator to all DOC IT systems, both national security and non-national security, to facilitate prioritization of resources. The Department defines three criticality levels: National Critical (critical infrastructure and key resources), Mission Critical (mission-specific or agency-specific systems), and Business Essential (agency-common support systems).

National Critical systems are systems where the mission served by the system, or the information that it processes affect the security of critical national infrastructures or key resources. Only the DOC Critical Information Assurance Officer (CIAO) (the DOC CIO) has authority within Commerce to officially designate a system as national critical. New systems must be approved by the Commerce IT Review Board (CITRB), which is chaired by the DOC CIO. The Exhibit 300 Business Case, presented to the CITRB by the system owner, requires description of the system criticality, including whether or not the system supports national critical functions. Through the CITRB, new national critical systems are identified and so designated by the CIAO.

Mission critical systems are associated with an agency's mission-specific or agency-specific activities and often vary from agency to agency. These systems support services to citizens and modes of delivery functions. In contrast, business essential systems support activities common to most agencies, and are associated with support services and management of agency resources.

### When are units required to submit updated IT system inventory?

Each operating unit must submit a copy of its IT system inventory to the Department's IT Security Program Manager semiannually (March 15 and September 15), which shows the security status of every system. Units must also provide updated inventories when significant changes occur to the status of their overall program or an individual system. In addition, operating units should provide interim updates when systems are added to or removed from the inventory, and at least monthly (by the 15$^{th}$ of the month) when undergoing significant changes to inventory data.

### When should systems be considered in the disposal or deactivated phase of the System Life Cycle?

Disposed or deactivated systems have effectively reached the final phase in the system life cycle as the system is defined in the IT System Inventory. For systems that have transferred or migrated functionality or data into another system (i.e., the system was consolidated into another system), some of the environment, management, and operational information from the SSPCAP might still be relevant for incorporation into the follow-on system SSPCAP. For systems that have become obsolete or are no longer in use, the system owner has effectively sanitized the system (of sensitive data and copyrighted material), and has properly archived data qualifying as federal records.

### What information is required to be maintained in the IT system inventory for disposed or deactivated systems?

Operating units must report disposed or deactivated systems once to the Department, with their semiannual inventory update for the mandated reporting period following system deactivation. All applicable fields in all tables, including the deactivation date field, must be completed for that system inventory update. Operating units must insert "n/a" into fields in the Security Information and System Interconnections Tables, to reflect that the operational system security compliance requirements no longer apply. Where system boundaries have been redefined, resulting in "deactivation" of a system in the inventory, annotate in the System Name field the name of the new or existing "parent" system (e.g., "Sys-001, System 1 – consolidated into Sys-005"). This notation in the System Name field will facilitate audit work by indicating "where" the system went in instances where it was not actually disposed of and is instead still in use under a new system boundary. The operating unit should not re-issue the System ID number, and must archive the last System Security Certification and Accreditation Package and associated system disposal records for audit purposes, for a period of at least 2 years to be able to respond to Departmental and external reviews of system disposal practices.

The Department IT Security Program Team shall maintain copies of historical inventory data, including the final report of deactivated systems, in accordance with Federal and Departmental record keeping requirements – but at least 2 years. Units that require a listing of their deactivated systems can request them from the Department during the 2-year period of record retention. The historical information will be retained in the Department's database for audit purposes as auditors often will inquire about deactivated systems and the procedures for accounting for them and procedures for disposal (e.g., auditors may request a report from the inventory of deactivated systems and then go to the operating unit to review system sanitization/data erasure procedures).

### How do I determine the Baseline Security Controls (BSC) System Impact Level?

To determine the value for the BSC system impact level inventory data field, you must first understand the potential impact level values, establish the potential impact levels for each *information type*, and then establish the potential impact level for the *information system*, using criteria contained in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*.

- Understanding the potential Impact Level determinations: The potential impact level may vary depending on other factors associated with the system and this amplification, as described below. Assignment of a specific impact level requires the judgment of system owners and other responsible program officials.
  - The *potential impact* is **HIGH** if——The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. *AMPLIFICATION*: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major

financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

- The *potential impact* is **MODERATE** if—– The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. *AMPLIFICATION*: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
- The *potential impact* is **LOW** if—The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. *AMPLIFICATION*: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

- Determine potential impact levels for each *information type*: Begin with determining the potential impact level (low, moderate, or high) for each of the stated *security objectives* (confidentiality, integrity, and availability) for each *type* of information stored in or processed by the system. The security category (SC) of each *information type* is represented as a triple of the associated potential impacts for each *security objective*. The FIPS 199 generalized format for expressing the SC of an *information type* is:

  **SC** information type= {(confidentiality, ***potential impact***), (integrity, ***potential impact***), (availability, ***potential impact***)},

  where the acceptable values for potential impact for each of the security objectives are LOW, MODERATE, or HIGH for the *information type*.

- Determine potential impact level for the *information system*: After determining the potential impact level for each *information type*, FIPS 199 further defines the *system impact level* as the maximum value (or high water mark) from among the impacts noted in the above formula for each *information type* on the system. That is: (i) if the highest potential impact for a *security objective* is LOW among all *information types* on the system, system impact level is LOW; (ii) if the highest potential impact for a *security objective* is MODERATE among all *information types* on the system, system impact level is MODERATE; and (iii) if the highest potential impact for a *security objective* is HIGH among all *information types* on the system, system impact level is HIGH. For example, the SC for an *information system* supporting an organization's acquisition process is expressed as:

  **SC** contract information = {(confidentiality, **MODERATE**), (integrity, **MODERATE**), (availability, **LOW**)},

  and

  **SC** administrative information = {(confidentiality, **LOW**), (integrity, **LOW**), (availability, **LOW**)}.

The resulting SC of the *information system* is expressed by selecting the maximum value (or high water mark) of the potential impacts from among the *information types* for each *security objective*:

**SC** acquisition system = {(confidentiality, **MODERATE**), (integrity, **MODERATE**), (availability, **LOW**)}.

- Determine the BSC System Impact Level: To determine the BSC System Impact Level, select the *highest value* of the potential impacts among the *security objectives* for the SC for the *information system*; that is: (i) if the highest potential impact is LOW, the BSC is LOW; (ii) if the highest potential impact is MODERATE, the BSC is MODERATE; and (iii) if the highest potential impact is HIGH, the BSC is HIGH. Using the above acquisition system example, the maximum value (or high water mark) of the potential impacts for the system is **MODERATE** and, therefore, the BSC of **MODERATE** is assigned.

## Where can I get help in completing the IT system inventory?

The data dictionary (attachment 1) and examples of properly completed inventory tables (attachment 2) further demonstrate proper completion of the inventory fields. Also, the operating unit may contact the DOC IT Security Program Team: Nancy DeFrancesco, Program Manager, (202) 482-3490, NDeFrancesco@doc.gov or Willie Graham, (202) 482-0273, WGraham@doc.gov, for assistance.

For more information on IT Capital Planning issues such as the Exhibit 300 and 53, see OMB Circular A-11, the DOC *IT Capital Asset Planning and Management Process*, and the DOC *Instructions for Completing the OMB Exhibit 300,Capital Asset Plan and Business Case*.

## DOC IT System Inventory Data Dictionary

The IT System Inventory database is segmented into four tables, as described in detail below.



---

### System Description Table (SYSDESC)

Table Description: In the System Description Table, each field represents information that identifies each system. Examples are system identification number, system location, and the system type. This information must reflect the information described in the IT System Security Plan for the system. *(A = Alphanumeric in the format area)*

| Field Name | Format | Field Description |
|---|---|---|
| SysID | A15 | System Identification Number (PRIMARY KEY)<br>The system identification number is the operating unit's CIO-assigned identifier number, containing the acronym for the unit and a three or four digit number for each IT system. This number must be unique to that system. |
| SysName | A120 | System Name<br>The system name/title describes each IT system uniquely. If the system is an aggregation of systems, ensure that "Aggregate" is included in the system name. Always spell out the complete name of the system, and do not use acronyms. A system is identified by defining boundaries around a set of processes, communications, storage, and related resources, as defined in NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*. The elements within these boundaries constitute a single system requiring a system security plan and a security evaluation whenever a major modification to the system occurs. Each element of the system must be under the same direct management control; have the same function or mission objective; have essentially the same operating characteristics and security needs; and reside in the same general operating environment. Furthermore, each system in the inventory is subject to all Federal and Departmental policies pertaining to IT security. |

| Field Name | Format | Field Description |
|---|---|---|
| SensitiveType | A25 | Sensitivity Type<br>The sensitivity type identifies whether the system is a national security system or not a national security system. Guidance for identifying national security systems is provided in FISMA and is further defined in NIST Special Publication 800-59, *Guideline for Identifying an Information Systems as a National Security System*. Inventory values are:<br>**PAU** = Publicly available unclassified non-national security (government information available to the public)<br>**SBU** = Sensitive-but-unclassified non-national security (private data, Sensitive/Limited Official Use Only information, or other proprietary information)<br>**NSU** = National security-But-Unclassified<br>**NSC** = National security-Classified confidential<br>**NSS** = National security-Classified secret<br>**NSTS** = National security-Classified top secret |
| SysLoc | A70 | System Location<br>The system's physical location (city, building, and, room number) |
| SysType | A25 | System type<br>This field identifies each system as either a "major application" (MA) or a "general support system" (GSS). Systems will be covered individually if they have been designated either as a MA or within the security plan of a GSS that identifies applications served by the GSS. Values are:<br>**GSS** = General support system: An interconnected set of information resources under the same direct management control and operating environment, and that shares common functionality.<br>**MA** = Major application: A major application is an application that requires special attention to security due to the risk and magnitude of the harm, and can be either a major software application or a combination of hardware/ software where the only purpose of the system is to support a specific mission-related function. |
| LifeCycle | A25 | Life Cycle Stage<br>This field identifies the life cycle management stage of the system. Values are:<br>**IN** = Initiation |

| Field Name | Format | Field Description |
|---|---|---|
| | | **DA** = Development/Acquisition<br>**IM** = Implementation<br>**OM** = Operation & Maintenance<br>**D** = Disposal/Deactivation |
| DeactDate | mm/dd/yyy | Deactivation date<br>This field contains the date that the system was deactivated or disposed, and no longer approved for processing information. |
| SysCrit | A25 | System criticality<br>The system criticality field is defined by the need for a system, and its information, to be available to support Government-wide, Department-wide, or operating unit processes, and is based on the type of information stored in, processed by, or generated by that system as described in draft NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categorization Levels*. Values are:<br>**NC** = National Critical systems are only designated by the DOC CIAO (the Department CIO), and are deemed critical infrastructure and key resources that must be restored in 72 hours.<br>**MC** = Mission Critical systems are mission-specific or operating unit-specific systems that often vary from unit to unit.<br>**BE** = Business Essential systems support activities common to most operating units, and are associated with support services and management of agency resources. |
| Exb53/300AcctCd | A50 | Exhibit 53/300 Account Code<br>The *Unique Project Identifier* (UPI) account code placed on Exhibit's 53 and 300 to report the investment during the budget year. The UPI depicts the agency code, bureau code, mission area (where appropriate), part of the exhibit where the investment will be reported, type of investment, agency four-digit identifier, year the investment entered the budget, and mapping to the Federal Enterprise Architecture. See OMB Circular A-11, for additional information on UPI codes. |
| BSCSImpactLvl | A8 | Baseline Security Controls (BSC) System Impact Level<br>To determine the BSC system impact level, begin with determining the potential levels of impact (low, moderate, |

| Field Name | Format | Field Description |
|---|---|---|
| | | and high) for each of the stated security objectives (confidentiality, integrity, and availability) for each type of information stored in or processed by the system using criteria in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. After determining the potential impact level for each information type, use the FIPS 199 criteria to determine the *system impact level*. The FIPS 100 criteria are explained on page 5 of the DOC *Process Guidance and Minimum Implementation Standards for IT System Inventory Management*. Finally, select the highest value of the potential impacts from among the three security objectives; that is: (i) if the highest potential impact is *Low*, the BSC system impact level is LOW; (ii) if the highest potential impact is *Moderate*, the BSC system impact level is MODERATE; and (iii) if the highest potential impact level is *High*, the BSC system impact level is HIGH. Values are:<br>Low<br>Moderate<br>High |
| GOCOEquip | A4 | System Equipment Ownership<br>Indicate whether the system is operated on government or contractor equipment. Values are:<br>GFE = Government-owned/furnished equipment<br>COE = Contractor-owned equipment |
| GOCOFac | A4 | System Facility Ownership/Lease<br>Indicate whether the system is operated in a government or contractor facility. Values are:<br>GF = Government-owned/leased facility<br>CF = Contractor-owned/leased facility |
| OpsPers | A4 | System Operations Personnel<br>Indicate whether federal government or contractor personnel operate the system. Values are:<br>F = Operated by government personnel<br>C = Operated by contractor personnel<br>FC = Operated by a combination of both government and contractor personnel, with full-time on-site federal personnel overseeing the daily work of contractors. |

*(End System Description Table Data Dictionary)*

## System Responsibility Table (SYSRESP)

**Table Description:** In the System Responsibility Table, each field represents individuals who are responsible for the security of each system. Examples are system security officer, system owner, and designated approving authority. This information must reflect the information described in the IT System Security Plan for the system. *(A = Alphanumeric in the format area)*

| Field Name | Format | Field Description |
|---|---|---|
| SysID | A15 | System Identification Number (PRIMARY FIELD)<br>The system identification number is an operating unit's CIO-assigned identifier number, containing the acronym for the unit and a three or four digit number for each IT system. This number must be unique to that system. |
| SecOfficer | A70 | Security Officer<br>Name and phone of the person assigned operational security responsibility (e.g., the information system security officer or system owner if no ISSO has been assigned) |
| SysOwner | A70 | System Owner<br>Name and phone number of the system owner who is responsible for day-to-day system operations |
| DAA | A70 | Designated Approving Authority<br>Name and phone number of the designated approving authority (operating unit head or lead program official) authorized to accredit the system for operation. |

*(End System Responsibility Table Data Dictionary)*

## Security Information Table (SECINFO)

**Table Description:** In the Security Information Table, each field represents current system security information that overall reflect the status of an operating unit's implementation of its IT Security Program. Examples are security plan date, risk assessment date, and accreditation date. This information must reflect the information described in the IT System Security Plan for the system. *(A = Alphanumeric in the format area)*

| Field Name | Format | Field Description |
|---|---|---|
| SysID | A15 | System Identification Number (PRIMARY FIELD)<br>The system identification number is an operating unit's CIO-assigned identifier number, containing the acronym for the unit and a three or four digit number for each IT system. This number must be unique to that system. |
| SSPCAPFoll | A5 | SSPCAP Followed?<br>Whether the DOC System Security Plan Certification and Accreditation Process (SSPCAP) methodology was followed for the system certification and accreditation. The SSPCAP is consistent with methodologies described in NIACAP (for national security systems) and NIST Special Publication 800-37 (for non-national security system). Values are:<br>**Y** = Yes<br>**N** = No |
| LevOfEffort | A5 | Level of Effort *(NOTE: Changes in testing are to be applied to C&A efforts **started after** the effective date of this standards change)*<br>The level of effort and resources applied to the certification and accreditation of an IT system. Values are:<br>**1** = Level 1: Checklist (NIST 800-26)<br>**2** = Level 2: Abbreviated (Level 1 plus internal system vulnerability scan testing)<br>**3** = Level 3: Moderate (Level 2 plus external system vulnerability scan testing and external penetration testing required for systems of High System Impact Level, optional for systems of Moderate and Low Impact)<br>**4** = Level 4: Extensive [Level 3 plus external (for systems of High, Moderate, and Low System Impact Level) and internal penetration testing] |
| SecPlanDt | mm/dd/yyyy | Security Plan Date<br>Date the system owner most recently approved the security plan |

| Field Name | Format | Field Description |
|---|---|---|
| RiskAssDt | mm/dd/yyyy | Risk Assessment Date<br>Date of the last system security risk assessment |
| ContPlanDt | mm/dd/yyyy | Contingency Plan Date<br>Date the contingency plan was most recently updated |
| ContPlanTestDt | mm/dd/yyyy | Contingency Plan Test Date<br>Date the contingency plan was last tested |
| ST&EPlan | A5 | ST&E Plan?<br>Whether a security test & evaluation (ST&E) plan was developed during system certification. Values are:<br>**Y** = Yes<br>**N** = No |
| ST&EPlanTestDt | mm/dd/yyyy | ST&E Plan Testing Completion Date<br>Date last ST&E plan testing was completed |
| CertDt | mm/dd/yyyy | Certification Date<br>Date of the certifier's recommendation regarding the adequacy of management, operational, and technical security controls of a system; and the effectiveness of those controls to mitigate risk to an acceptable level |
| AccredDt | mm/dd/yyyy | Accreditation Date<br>Date the accrediting program official most recently approved the system for operation |
| AccredType | A10 | Accreditation Type *(NOTE: Changes in Types are to be applied to accreditations issued **after** the effective date of this standards change)*<br>The type of accreditation issued by the accrediting program official. Values are defined in NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. Inventory values are:<br>**A** = Authorization to operate (for systems accredited after the effective date of this policy and standards change)<br>**F** = Full Accreditation (for system accreditations prior to effective date of this policy and standards change only)<br>**I** = Interim authorization to operate<br>**D** = Denial of authorization to operate |
| SelfAssDt | mm/dd/yyyy | Self Assessment Date<br>Date most recent self-assessment (in accordance with NIST Special Publication 800-26 guidance) was completed |

| Field Name | Format | Field Description |
|---|---|---|
| AuditDt1 | mm/dd/yyyy | Audit Date 1<br>Date of most recent evaluation or audit performed by an external organization within the last 24 months (should match to Audit Organization 1 and Audit Report Number 1) |
| AuditDt2 | mm/dd/yyyy | Audit Date 2\<br>Date of second most recent evaluation or audit performed by an external organization within the last 24 months (should match to Audit Organization 2 and Audit Report Number 2) |
| AuditDt3 | mm/dd/yyyy | Audit Date 3<br>Date of third most recent evaluation or audit performed by an external organization within the last 24 months (should match to Audit Organization 3 and Audit Report Number 3) |
| AuditOrg1 | A15 | Audit Organization 1<br>Name of the external organization that conducted the most recent evaluation or audit (e.g., OIG, GAO, DOC) within last 24 months (should match to Audit Date 1 and Audit Report Number 1) |
| AuditOrg2 | A15 | Audit Organization 2<br>Name of the external organization that conducted the second most recent evaluation or audit within last 24 months (should match to Audit Date 2 and Audit Report Number 2) |
| AuditOrg3 | A15 | Audit Organization 3<br>Name of the external organization that conducted the third most recent evaluation or audit within last 24 months (should match to Audit Date 3 and Audit Report Number 3) |
| AuditReptNo1 | A15 | Audit Report Number 1<br>Report number for most recent evaluation or audit performed by external organizations within last 24 months (should match to Audit Date 1 and Audit Organization 1) |
| AuditReptNo2 | A15 | Audit Report Number 2<br>Report number for second most recent evaluation or audit performed by external organizations within last 24 months (should match to Audit Date 2 and Audit Organization 2) |
| AuditReptNo3 | A15 | Audit Report Number 3<br>Report number for third most recent evaluation or audit performed by external organizations within last 24 months (should match to Audit Date 3 and Audit Organization 3) |

*(End Security Information Table Data Dictionary)*

**System Interconnections Table (SYSCONNECT)**

**Table Description:** In the System Interconnection Table, each field represents current information that identifies the interfaces between the operating unit's system and all other systems or networks not covered by the same security plan, including those not operated by or under the control of the Department. Examples are the name of the organization the connection is with and the interconnected system's number or the name. Systems in the DOC IT System Inventory may have many different system interconnections – to other DOC systems, to the Internet, to business partners, and to other government agencies. List each different interconnection separately in this table. These interconnections must reflect the information described in the System Interconnection/Information Sharing section of the IT System Security Plan for the system. (A = Alphanumeric in the format area)

| Field Name | Format | Field Description |
|---|---|---|
| SysID | A15 | System Identification Number (PRIMARY FIELD)<br>The system identification number is an operating unit's CIO-assigned identifier number, containing the acronym for the unit and a three or four digit number for each IT system. This number must be unique to that system. |
| InterconnOrg | A50 | Interconnection Organization<br>The name of the entity/organization to which this system (identified by the DOC System Identifier above) is connected – for example, Department of Justice (DOJ), National Finance Center (NFC), DOC/National Oceanic and Atmospheric Administration (DOC/NOAA), or the Internet Service Provider business partner. Spell out all acronyms. For DOC operating units, be as specific as possible and include the line or program office title if known. |
| InterconnSysID | A50 | Interconnection System Identification or Name<br>The system identification number or name (if the system is not a DOC system) of the interconnected system – for example, a DOC system is identified by the system ID assigned by the owning operating unit's CIO; an external system may have a specific name such as the Civil Applicant System; or general connections to the Internet would have no specific name but would state "Internet." |
| InterconnTransType | A5 | Interconnection Transaction Type<br>The type of transaction supported by the interconnection. Values are:<br>G2G = Government-to-Government<br>G2B = Government-to-Business<br>G2C = Government-to-Citizen |

*(End System Interconnection Table Data Dictionary)*
*(End DOC IT System Inventory Database Data Dictionary)*

**Example of Properly Completed IT System Inventory Worksheet for the System Description Table Input**

| System ID Number | System Name/Title | Sensitivity Type | System Location | System Type | Life Cycle Stage | Deactivation Date | System Criticality | Exhibit 53/300 Account Code | System Impact Level | GOCO Equip | GOCO Fac | GOCO OpsPers |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DOC001 | Commerce Financial Management System | SBU | HCHB, Room 2 | MA | OM | | MC | 00800020001051107704139 | High | GFE | GF | F |
| DOC002 | Information Technology Investment Planning System | SBU | HCHB, Room 3 | MA | D | 03/23/2001 | MC | 0040001010267033000111 | Moderate | COE | CF | C |

**Example of Properly Completed IT System Inventory Worksheet for the Responsibility Table Input**

| System ID Number | Security Officer Name & Number | System Owner Name & Number | DAA Name & Number |
|---|---|---|---|
| DOC001 | Tom Smith, (301) 123-4567 | Dick Doe, (301) 234-5678 | Harry Jones, (301) 345-6789 |
| DOC002 | Tom Smith, (301) 123-4567 | Dick Doe, (301) 234-5678 | Harry Jones, (301) 345-6789 |

**Example of Properly Completed IT System Inventory Worksheet for the Security Information Table Input**

| System ID Number | NIACAP Followed | Level of Effort | Security Plan Date | Risk Assessment Date | Contingency Plan Date | Contingency Plan Test Date | ST&E Plan | ST&E Plan test Date | Certification Date | Accreditation date | Accred Type | Self-Assessment Date | Audit Date1 | Audit Organization1 | Audit Number1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DOC001 | Y | 3 | 09/15/2002 | 09/13/2002 | 06/01/2002 | 10/22/2003 | Y | 10/07/2002 | 10/08/2002 | 10/11/2002 | A | 07/17/2002 | 04/11/2002 | OIG | O893765 |
| DOC002 | Y | 3 | 03/06/2001 | 03/01/2001 | 02/11/2001 | 10/22/2003 | Y | 04/01/2001 | 04/03/2001 | 04/05/2001 | I | 07/17/2002 | 11/02/2001 | GAO | GAO-02-300 |

**Example of Properly Completed IT System Inventory Worksheet for the System Interconnections Table Input**

| System ID Number | Interconnected ORG | Interconnected DOC SYSID or Non-DOC System Name | Interconnected Transaction TYPE |
|---|---|---|---|
| DOC001 | DOC | DOC002 | G2G |
| DOC001 | Dept. of State (DOS) | DOS Secure Web Server | G2G |
| DOC001 | National Finance Center (NFC) | ABC Payroll System | G2G |
| DOC002 | UUNet | Internet | G2C |
| DOC002 | DOC | DOC0001 | G2G |